



PATENT APPLICATION

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re application of

Docket No: Q61823

Jae-han PARK

Appln. No.: 09/721,713

Group Art Unit: 2131

Confirmation No.: 4060

Examiner: Longbit CHAI

Filed: November 27, 2000

For: AUTHENTICATION METHOD FOR ESTABLISHING CONNECTION BETWEEN
DEVICES

SUBMISSION OF APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith please find an Appeal Brief.

Please charge the statutory fee of \$500.00 to Deposit Account No. 19-4880. The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account. A duplicate copy of this paper is attached.

Respectfully submitted,

Diallo T. Crenshaw
Registration No. 52,778

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: December 8, 2006



PATENT APPLICATION

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re application of

Docket No: Q61823

Jae-han PARK

Appln. No.: 09/721,713

Group Art Unit: 2131

Confirmation No.: 4060

Examiner: Longbit CHAI

Filed: November 27, 2000

For: AUTHENTICATION METHOD FOR ESTABLISHING CONNECTION BETWEEN
DEVICES

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant submits the following:

Table of Contents

I.	REAL PARTY IN INTEREST.....	2
II.	RELATED APPEALS AND INTERFERENCES	3
III.	STATUS OF CLAIMS.....	4
IV.	STATUS OF AMENDMENTS.....	5
V.	SUMMARY OF THE CLAIMED SUBJECT MATTER.....	6
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL	7
VII.	ARGUMENT.....	8
	CLAIMS APPENDIX	16
	EVIDENCE APPENDIX:	22
	RELATED PROCEEDINGS APPENDIX.....	23

12/11/06 15 01:12:00 01/02/07 154000 00721713

ON 03/14/02

01/02/07

I. REAL PARTY IN INTEREST

Based on the information supplied by the Appellant, and to the best of Appellant's legal representative's knowledge, the real party in interest is the assignee, SAMSUNG ELECTRONICS CO., LTD.

II. RELATED APPEALS AND INTERFERENCES

Appellant, as well as Appellant's assigns and legal representatives, are unaware of any appeals or interferences which will be directly affected by, or which directly affect or have a bearing on, the Board's decision in the pending case.

III. STATUS OF CLAIMS

Claims 1-14 are all the claims pending in the present application, have been finally rejected, and are the subject of this appeal. The pending claims are set forth in the Appendix.

IV. STATUS OF AMENDMENTS

No amendments have been made subsequent to the Final Office Action dated May 8, 2006.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

In an exemplary embodiment of the present invention, there is provided an authentication method for establishing a connection between devices that can wirelessly communicate data, the method including: (a) sending a first authentication-request message to another device to perform an authentication procedure with the other device to which a connection is wanted (e.g., S202 of FIG. 2- page 8, lines 5-9); (b) sending a predetermined message according to a current operation mode to the other device and storing the predetermined message (e.g., S228 of FIG. 2 - page 15, lines 15-20) when an authentication-response message (e.g., S204 of FIG. 2- page 8, line 18- page 9, line 9) to the first authentication-request message is received; (c) after performing the step (b), checking whether a received first message is a response message corresponding to the predetermined message when the first message from the other device is received (e.g., S232 OF FIG. 2- page 16, lines 15-20); (d) sending a response message corresponding to a second authentication-request message to the other device when the result of checking in the step (c) indicates that the first message is the second authentication-request message (e.g., S236 of FIG. 2 -page 16, line 1- page 17, line 6); (e) after performing the step (d), checking whether a second message is a response message corresponding to the predetermined message when the second message from the other device is received (e.g., S239 of FIG. 2- page 17, line 20- page 18, line 5); and (f) finishing the authentication procedure when the result of checking in the step (e) indicates that the second message is a response message corresponding to the predetermined message (e.g., S240 of FIG. 2- page 17, line 20- page 18, line 5). Other related embodiments are set forth in independent claims 7 and 12.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-14 stand rejected under 35 U.S.C. § 102(a) as allegedly being anticipated by Bluetooth (Specification of the Bluetooth System: The ad hoc SCATTERNET for affordable and highly functional wireless connectivity, vol. 1.0a, July 26, 1999).

VII. ARGUMENT

A. Rejection of Claims 1-6

With respect to independent claim 1, Appellant submits that Bluetooth does not teach or suggest at least, “(b) sending a predetermined message according to a current operation mode to the other device and storing the predetermined message when an authentication-response message to the first authentication-request message is received.” To support the rejection of claim 1, the Examiner previously cited Part C, Section 3.3.4, page 197 of Bluetooth as allegedly satisfying the above-quoted feature of claim 1. However, the cited portion of Bluetooth and other related portions of Bluetooth fail to teach or suggest that a predetermined message is sent according to a current operation mode. Further, Bluetooth does not teach or suggest that the predetermined message is stored when an authentication-response message to the first authentication-request message is received. The portion of Bluetooth cited by the Examiner only discusses the operation of creating a link key, and storing a link key in memory. Nowhere does Bluetooth even mention sending a predetermined message according to a current operation mode or that a sent predetermined message is, in fact, stored.

In the *Response to Arguments* section of the Office Action dated January 27, 2005, the Examiner alleges:

As per claim 1, Applicant asserts “Bluetooth fail to teach or suggest that a predetermined message is sent according to a current operation mode and is stored when an authentication-response message to the first authentication-request message is received”. However, the Examiner is interpreting, in Bluetooth, when the authentication is finished the link key must be created (Bluetooth: see for example, Part-C, Section 3.3.4, first sentence) and

subsequently the link key message is sent and the response message is received (Bluetooth: see for example, Part-C, Section 3.3.4 Figure/Sequence 7). The selection of the link key, either LMP_unit_key or LMP_comb_key, is determined based on whether response message received matches the message being sent or not - or more specifically, based on which message being sent and which message being received (between LMP_unit_key message and LMP_comb_key message) (Bluetooth: see, for example, Part-C, Section 3.3.4, page 198, bullets 1-3). Thereby, Examiner notes the predetermined message being sent is interpreted as the “key selection message” as addressed above and this predetermined message “must” be stored (inherently) so that the decision rule for key selection can be applied to compare the message being sent against the message being received/responded (Bluetooth: see for example, Part-C, Section 3.3.4, Lines 9-13, page 198, bullets 1-3).

In response, Appellant maintains that Bluetooth does not teach or suggest at least the above-quoted limitation at least based on the following reasons as well as those set forth above. First, Appellant submits that the Examiner has not established which messages in the Bluetooth reference allegedly correspond to the claimed 1) predetermined message, 2) first authentication-request message, and 3) authentication-response message. That is, the Examiner, in the *Response to Argument* Section, simply reiterates the teachings of the Bluetooth reference at the portions cited, however, the particular portions of the Bluetooth reference relied on by the Examiner (particularly Section 3.3.4, page 198) do not show messages that correspond to at least the three claimed messages set forth above. In Section 3.3.4, for example, only two signals are shown being sent between the verifier and claimant. Further, even if, *arguendo*, the Bluetooth reference does show, in some other section, three different signals being sent between a different verifier and claimant, there is no teaching or suggestion that the particular signals that are disclosed correspond to the claimed predetermined message, authentication-response message,

and first authentication-request message, as recited in claim 1. Yet further, the specific correlation between the claimed messages is not taught or suggested anywhere in Bluetooth. That is, nowhere does the Bluetooth reference teach or suggest that a predetermined message is stored when an authentication-response message to the first authentication request message is received, for example, as described in claim 1.

Yet even further, in response to the last sentence in the Examiner's argument above, Appellant submits that it is not inherent that a particular signal must be stored in order for a key selection to be made (see Section 3.3.4 of the Bluetooth reference). That is, in order to determine which key will be the link key (see top of page 198 of Bluetooth reference), a value associated with a received key can be retained, and that value could be used in determining a key to select as the "link key". However, it does not necessarily follow that a "key selection message" (which is a term used by Examiner) would have to be stored in order to compare received/response messages.

Further, with respect to claim 1, even if, *arguendo*, the Examiner identifies specific messages in the Bluetooth reference (in the Advisory Action dated May 20, 2005 and the Office Action dated January 11, 2005) which allegedly correspond to the claimed messages¹, the specific operations (c) and (d) of claim 1, for example, are not satisfied. Appellant submits that even if one substitutes the messages of the Bluetooth reference that allegedly correspond to the

¹ The Examiner alleges that: 1) the LMP_unit_key (or LMP_comb_key) message corresponds to the claimed "predetermined message", 2) the LMP_in_rand (or LMP_auth_rand) message corresponds to the claimed "first authentication-request message", and 3) the LMP_accepted (or LMP_not_accepted) message corresponds to the claimed "authentication response message".

claimed first authentication request message, predetermined message, and authentication response message, respectively, as recited in claim 1, the specific recitations set forth in claim 1 are still clearly not satisfied by Bluetooth. The Examiner is apparently utilizing impermissible hindsight reasoning, as the Examiner appears to be picking and choosing different portions of the applied reference to satisfy the specific features set forth in claim 1. By stepping through the recitations of claim 1, for example, it is evident that the Bluetooth reference does not satisfy the particular features set forth in claim 1.

Further, with respect to the operation (c) of claim 1, the Examiner appears to contradict himself with respect to this claim. That is, on page 6 of the Office Action dated January 27, 2005, the Examiner states that the Bluetooth reference does not teach operation (c) of claim 1. However, the Examiner now alleges that the Bluetooth reference does satisfy this particular feature. Thus, the Examiner's arguments do not appear to be consistent. Appellant submits that this inconsistency of arguments by the Examiner is a direct reflection of the fact that the Bluetooth reference does not satisfy at least operations (c) and (d) of claim 1.

Therefore, at least based on the foregoing, Appellant submits that independent claim 1, as well as dependent claims 2-6, would not have been anticipated by or rendered obvious in view of Bluetooth.

B. Rejection of claim 7-11, 13 and 14

With respect to independent claim 7, Appellant submits that Bluetooth does not teach or suggest, "(b) after performing the step (a) and prior to performing the step(c), checking an authentication condition of the present device when a predetermined message from the other

device is received; (c) after performing the step (b), storing the predetermined message and sending a second authentication-request message to the other device when the result of checking indicates that a mutual authentication is required.” As similarly set forth above with respect to claim 1, Appellant submits that the Examiner has not identified what messages allegedly correspond to the claimed predetermined message, second authentication-request message, and response message, as set forth in claim 7. That is, the Examiner cannot make a plausible argument that the above-quoted operations of the present invention, as recited in claim 7, are satisfied by Bluetooth because the Examiner has not identified the particular messages that allegedly correspond to the messages claimed in claim 7. Therefore, at least based on the foregoing, Appellant maintains that Bluetooth does not teach or suggest the above-quoted limitation of claim 7.

Further, with respect to claim 7, the Examiner is yet again inconsistent in his arguments, as the Examiner previously stated that Bluetooth does not satisfy the feature, “after performing the step (a) and prior to performing the step(c), checking an authentication condition of the present device when a predetermined message from the other device is received,” because the Bluetooth reference does not expressly disclose how to determine the authentication condition. However, the Examiner now alleges that the Bluetooth reference satisfies the above-quoted feature. Hence, the inconsistent argument.

Accordingly, Appellant submits that independent claim 7, as well as dependent claims 8-11, 13 and 14, would not have been anticipated by or rendered obvious in view Bluetooth.

C. Rejection of claim 12

With respect to independent claim 12, Appellant submits that Bluetooth does not disclose or suggest, “determining whether an authentication procedure for establishing a connection between the devices...is performed as a unilateral authentication procedure or as a mutual authentication procedure, according to an authentication condition which enables receiving an authentication request in the two devices that can communicate data,” as recited in claim 12. Appellant believes that this claim is patentable over Bluetooth based on reasons similar to those set forth above with respect to claims 1 and 7. In particular, Appellant submits that the Examiner has not identified what messages in Bluetooth allegedly correspond to the claimed operation of determining whether an authentication procedure for establishing a connection between the devices...is performed as a unilateral authentication procedure or as a mutual authentication procedure. Yet further, Appellant submits that the Examiner has not identified which aspects of Bluetooth allegedly correspond to the claimed authentication condition which enables receiving an authentication request in the two devices that can communicate data. That is, the Examiner cannot make a plausible argument that the above-quoted operation of the present invention, as recited in claim 12, is satisfied by Bluetooth because the Examiner has not identified the particular messages of Bluetooth that allegedly correspond to the specific features of claim 7 discussed above.

Further, Appellant respectfully points out to the Board of Patent Appeals and Interferences that the Examiner initially acknowledged that Bluetooth fails to teach the above quoted feature of claim 12.

Finally, in the Advisory Action dated August 18, 2006, the Examiner alleges, in part:

Applicants maintain that even if one substitutes the messages of the Bluetooth that allegedly correspond to the claimed first authentication request message, predetermined message, and authentication response message, respectively, as recited in claim 1, the specific recitations set forth in claim 1 are still clearly not satisfied by Bluetooth. Examiner respectfully disagrees. Examiner notes Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the art disclosed by the references cited or the objections made. Further, they do not show how the amends avoid such reference or objections.

Appellant has pointed out the patentable novelty of the claimed invention over Bluetooth in several of the previous Amendments/Responses and have identified the specific features of the claimed invention that render the claimed invention distinguishable over the prior art. In the most recent Response filed August 8, 2006, in an effort to assist the Examiner in understanding the differences between the present invention and Bluetooth, Appellant identified exemplary portions of the figures that correspond to the claimed features. These same exemplary corresponding portions of Fig. 2 and the specification are set forth in the Summary of the Claimed Subject Matter section of the present Appeal Brief. Even though the specific features of the claims were not repeated in the August 8th Response, these specific features and arguments were previously presented in previous Amendments/Responses. Therefore, Appellant submits that the patentably novelty has been demonstrated under 37 C.F.R. § 1.111(c).

Conclusion

Appellant submits, at least based on the foregoing, that Bluetooth does not anticipate the present invention, as recited in claims 1-14.

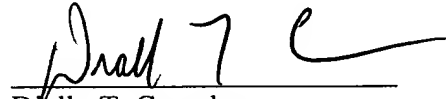
APPEAL BRIEF
USSN 09/721,713

ATTORNEY DOCKET NO. Q61823

Unless a check is submitted herewith for the fee required under 37 C.F.R. §41.37(a) and 1.17(c), please charge said fee to Deposit Account No. 19-4880.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Drallo T. Crenshaw
Registration No. 52,778

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: December 8, 2006

CLAIMS APPENDIX

CLAIMS 1-14 ON APPEAL:

1. An authentication method for establishing a connection between devices that can wirelessly communicate data, the method comprising the steps of:

(a) sending a first authentication-request message to another device to perform an authentication procedure with the other device to which a connection is wanted;

(b) sending a predetermined message according to a current operation mode to the other device and storing the predetermined message when an authentication-response message to the first authentication-request message is received;

(c) after performing the step (b), checking whether a received first message is a response message corresponding to the predetermined message when the first message from the other device is received;

(d) sending a response message corresponding to a second authentication-request message to the other device when the result of checking in the step (c) indicates that the first message is the second authentication-request message;

(e) after performing the step (d), checking whether a second message is a response message corresponding to the predetermined message when the second message from the other device is received; and

(f) finishing the authentication procedure when the result of checking in the step (e) indicates that the second message is a response message corresponding to the predetermined message.

2. The authentication method of claim 1, wherein in the step (b), when the current operation mode is a pairing process, a message for generating a link key is sent as the predetermined message and stored, and when the current operation mode is not a pairing process, a message of connection-establishment-completion is sent as the predetermined message and stored; and the step (f) further comprises the sub-steps of:

(f1) generating a link key before finishing the authentication procedure when the current operation mode is a pairing process; and

(f2) finishing the authentication procedure and establishing a connection to the other device when the current operation mode is not a pairing process.

3. The authentication method of claim 1, wherein the step (b) further comprises the sub-steps of:

(b1) checking whether the authentication-response message is valid using key information and random information; and

(b2) processing an authentication failure when the result of checking in the step (b1) indicates that the authentication-response message is not valid.

4. The authentication method of claim 3, wherein in the step (b1), the key information is held by the present device and the random information was used in sending the first authentication message.

5. The authentication method of claim 1, further comprising the step of:

(g) finishing the authentication procedure when the result of checking in the step (c) indicates that the received first message is a response message corresponding to the predetermined message.

6. The authentication method of claim 4, wherein in the step (b), when the current operation mode is a pairing process, a message for generating a link key is sent as the predetermined message and stored, and when the current operation mode is not a pairing process, a message of connection-establishment-completion is sent as the predetermined message and stored; and

the step (g) further comprises the sub-steps of:

(g1) generating a link key before finishing the authentication procedure when the current operation mode is a pairing process; and

(g2) finishing the authentication procedure and establishing a connection to the other device when the current operation mode is not a pairing process.

7. An authentication method for establishing a connection between devices that can wirelessly communicate data, the method comprising the steps of:

(a) sending a response message corresponding to a first authentication-request message when the first authentication-request message from another device that wants to establish a connection is received;

(b) after performing the step (a) and prior to performing the step(c), checking an authentication condition of the present device when a predetermined message from the other device is received;

(c) after performing the step (b), storing the predetermined message and sending a second authentication-request message to the other device when the result of checking indicates that a mutual authentication is required; and

(d) after performing the step (c), sending a response message corresponding to the message stored in the step (c) to the other device when a response message from the other device corresponding to the second authentication-request message is received, and finishing the authentication procedure.

8. The authentication method of claim 6, wherein in the step (d),
when the predetermined message received in the step (b) is a message for generating a link key, the present device sends a response message corresponding to the message for generating a link key to the other device, generates a link key, and then finishes the authentication procedure; and

when the predetermined message received in the step (b) is a message of connection-establishment-completion, the present device sends a response message corresponding to the message of connection-establishment-completion to the other device, finishes the authentication procedure, and then establishes a connection to the other device.

9. The authentication method of claim 6, wherein the step (d) further comprises the sub-steps of:

(d1) checking whether the response message corresponding to the second authentication-request message is valid when the response message corresponding to the second authentication-request message is received by using random information and key information; and

(d2) processing an authentication failure when the result of checking in the step (d1) indicates that the response message is not valid.

10. The authentication method of claim 9, wherein in the step (d1), the present device holds the key information and the random information was used in sending the first authentication message.

11. The authentication method of claim 6, wherein in the step (b) authentication enable information is checked as the authentication condition.

12. An authentication method for establishing a connection between devices that can wirelessly communicate data, the method comprising:

determining whether an authentication procedure for establishing a connection between devices that want to communicate data is performed as a unilateral authentication procedure or as a mutual authentication procedure, according to an authentication condition which enables receiving an authentication request in the two devices that can communicate data; and performing the authentication procedure.

13. The authentication method of claim 10, wherein in performing the authentication procedure, when the authentication condition of the device that receives the authentication request is set to require the mutual authentication procedure, the mutual authentication procedure

is performed by sending an authentication request message to the device that requests an authentication.

14. The authentication method of claim 10, wherein in performing the authentication procedure, the authentication procedure is determined by checking authentication enable information of the device that receives the authentication request.

APPEAL BRIEF
USSN 09/721,713

ATTORNEY DOCKET NO. Q61823

EVIDENCE APPENDIX:

There has been no evidence submitted pursuant to 37 C.F.R. § § 1.130, 1.131, or 1.132 or any other similar evidence.

APPEAL BRIEF
USSN 09/721,713

ATTORNEY DOCKET NO. Q61823

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.